SECURITY BULLETIN – bash shell arbitrary execution – Bulletin Version 1.7

Security Advisory Relating to *Bash* shell arbitrary code execution on Various Polycom Products.

DATE PUBLISHED: October 24, 2014

This information would apply only to all Polycom products that incorporate a *Bash* shell. Polycom is conducting ongoing research to determine the level of vulnerability (if any) for each of its various products.

Any information in this bulletin is subject to change.

Please Note: This is a living document, updated regularly until any product affected by any of the vulnerabilities in this bulletin has been repaired against that vulnerability. The newest version of this document will always reside at the following URL:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

Vulnerability Summary – NEW CVE's discovered

Two vulnerabilities in the GNU Bash shell allow for the execution of arbitrary code. Note that a partial fix was enacted to address the first vulnerability in the GNU Bash shell that inadvertently produced its own vulnerability. Both vulnerabilities involve the processing of environment variables and/or their values.

Details

CVE-2014-6271, aka "Shellshock"

In GNU *Bash* versions 4.3 bash43-025 and prior, an exploit of environment variable mechanics with regards to trailing strings allows the attacker to bypass or override environmental restrictions and run arbitrary code.

CVE-2014-6277

In GNU *Bash* versions 4.3 bash43-025 and prior, an exploit of environment variable mechanics with regards to function definitions allows the attacker to bypass or override environmental restrictions and run arbitrary code.

CVE-2014-7169

GNU *Bash* versions 4.3 bash43-025 and prior process environment variable values in a way that allows trailing strings to be added by an attacker, thus allowing the execution of arbitrary code.

CVE-2014-7186, aka "redir_stack" issue

parse.y in GNU *Bash* versions through 4.3 bash43-026 allows remote attackers to cause a denial of service (application crash) caused by a redirection implementation error (out-of-bounds array).

CVE-2014-7187, aka "word_lineo" issue

parse.y in GNU *Bash* versions through 4.3 bash43-026 allows remote attackers to cause a denial of service (application crash) caused by an off-by-one error in the read_token_word function (out-of-bounds array).

General Mitigations

Please read and understand these two mitigation sections before reading about which products are affected, and which come with their own internal mitigations:

Remembering that there are many attack vectors by which this vulnerability can be exploited, any sound mitigation must address this multiplicity of vectors. As well it is important to note that no matter which specific vector is under consideration, there are many possible means of mitigation: Polycom might have mitigated a specific vector on a specific product via programmatic means internal to the product, but it could just as easily be mitigated by a fielding condition. For example, turning off a given service might shut down a vector altogether.

An effective mitigation solution will incorporate strategies both from within the product and within the deployment architecture.

"Shellshock" (Bash vulnerability) is currently exploited via four known possible attack vectors. Note that a given product may or may not support one or all of these attack vectors:

1. Manipulating CGI calls into the target's HTTP server
2. Logging into the target via SSH to the Bash shell
3. Target's DCHP client connects to a malicious server
4. Inserting malicious strings into the target's SIP stack

Fielding/Deployment Mitigations per Vector

For HTTP, restrict web management access via the whitelist feature on the Polycom product where supported. Whitelisting can also be implemented on the network itself. Network segregation can also isolate all HTTP traffic to known and trusted entities. Additionally, web access can be disabled altogether if the fielding conditions permit.

For SSH, disable shell access. If shell access must be maintained, similar methods to those used above for HTTP may also be deployed (whitelisting, network segregation).

The DHCP client attack vector can be mitigated simply by setting all IP addresses manually (static addresses). When possible, one can also disable DHCP. It is generally good security guidance on infrastructure products to use static addresses anyway. Since no Polycom endpoints (audio or video) are vulnerable to Shellshock, they may continue to use DHCP without concern. Additionally, ensuring that the only DHCP server on the network is non-malicious (via network or other controls) can mitigate this vector.

For SIP, SIP Authentication can be used to associate all clients with known identities. Network controls such as IDS and IPS can be used. Firewall rules can be monitored for suspicious behavior. H.323 can also be used in lieu of SIP. Network Access Control Lists can be used as either blacklists or whitelists. SIP networks can be segregated.

Products Affected

Note that products in this table are the products whose vulnerability status can be spoken to at this time – to the positive or the negative. Products not listed in this chart should be considered under investigation.

RMX 1000 and 500	Not Vulnerable
CMA – All Versions	Not Vulnerable
RealPresence Desktop – All Versions	Not Vulnerable
RealPresence Mobile – All Versions	Not Vulnerable
Media Manager – All Versions	Not Vulnerable
CMAD (CMA Desktop) – All Versions	Not Vulnerable
CX Product Line, All Video Versions	Not Vulnerable
HDX – All Versions	Not Vulnerable
Group Series – All Versions	Not Vulnerable
Capture Station – All Versions	Not Vulnerable
CX Product Line, All Audio Versions	Not Vulnerable
RMX 4000, 2000 and 1500	Not Vulnerable
VVX Phones (w/ and w/out video) – All Versions	Not Vulnerable
SoundPoint Phones – All Versions	Not Vulnerable
SoundStation Phones – All Versions	Not Vulnerable
VSX – All Versions, Including V700 and V500	Not Vulnerable
CSS Client – All Versions	Not Vulnerable
SoundStructure	Not Vulnerable
OTX and RPX Immersive Telepresence	Not Vulnerable
Viewstation Family, Including FX	Not Vulnerable
PTC – Group Series & HDX Versions	Not Vulnerable
MGC Family	Not Vulnerable
RSS 2000	Not Vulnerable
CloudAXIS Experience Portal/Service Portal	Vulnerable – See Below Bash Upgrade mid-November

Distributed Media Application	FIXED in 6.0.1_P2_HF1 6.1.1_P1_HF1
Recording and Streaming Server 4000	Vulnerable – See Below Bash Upgrade Date Unknown
Video Border Proxy	**FIXED in 11.2.19**
RealPresence Access Director	Vulnerable – See Below Bash Upgrade in Q4 – v4.1.0
Platform Director	Vulnerable – See Below Bash Upgrade Date Unknown
CSS Gateway & Server	Vulnerable – See Below Bash Upgrade December
Collaboration Server 1800	Vulnerable – See Below Bash Upgrade in Q4 – v8.4.2
RealPresence Resource Manager	Vulnerable – See Below Bash Upgrade in Q4 – v8.3
Resource Manager Virtual Edition	Vulnerable – See Below Bash Upgrade in Q4 – v8.3
Capture Server	Vulnerable – See Below Bash Upgrade Date Unknown
Collaboration Server Virtual Edition	Vulnerable – See Below Bash Upgrade in Q4 – v8.4.2

Known Product-Specific Internal Mitigations

CloudAXIS Experience Portal and Service Portal:

Web – not vulnerable (web server does not set environment variables)
SIP – not vulnerable (stack tested by security team)
DHCP - vulnerable (DHCP client does not implement DHCP addresses received, but does “fetch” them for the VM’s)
SSH – Vulnerable (use of a restricted shell actually causes vulnerability in this place)

Distributed Media Application:

Web – not vulnerable (web server does not set environment variables)
SIP – not vulnerable (stack tested by security team)
DHCP – not vulnerable (DMA does not use DHCP)
SSH – vulnerable (can be disabled)

Recording and Streaming Server 4000:

Web – not vulnerable (web server does not set environment variables)
SIP – not vulnerable (stack tested by security team)

DHCP – vulnerable (set static addresses)
SSH – not vulnerable (no SSH capability)

RealPresence Access Director:

Web – not vulnerable (web server does not set environment variables)
SIP – Not vulnerable (SIP is Java implementation that does not use environment variables)
DHCP – presumed vulnerable, not tested (disable and use static address)
SSH – vulnerable (turn off)

Platform Director:

Web – not vulnerable (web server does not support CGI)
SIP – not vulnerable (no SIP stack)
DHCP – vulnerable (turn off and use static address)
SSH – vulnerable (but limited to the one root account)

CSS Gateway & Server:

Web – presumed not vulnerable, not tested
SIP – presumed not vulnerable, not tested
DHCP – vulnerable (turn off)
SSH – presumed not vulnerable, not tested

Collaboration Server 1800:

Web – not vulnerable (no Apache CGI)
SIP – not vulnerable (SIP stack does not interface with environment variables)
DHCP – presumed not vulnerable (only fires once during out-of-box)
SSH – vulnerable (off by default, should not be turned on)

RealPresence Resource Manager:

Web – not vulnerable (web server does not set environment variables)
SIP – not vulnerable, no SIP stack
DHCP – vulnerable (turn off and use static address)
SSH – vulnerable (turn off)

Resource Manager Virtual Edition:

Web – not vulnerable (web server does not set environment variables)
SIP – not vulnerable, no SIP stack
DHCP – presumed vulnerable, not tested (turn off and use static address)
SSH – presumed vulnerable, not tested (turn off)

Capture Server:

Web – presumed vulnerable, not tested
SIP – presumed vulnerable, not tested
DHCP – vulnerable (turn off, use static address)
SSH – presumed vulnerable, not tested

Collaboration Server Virtual Edition:

Web – not vulnerable (no Apache CGI)
SIP – not vulnerable (SIP stack does not interface with environment variables)
DHCP – presumed not vulnerable (DHCP during setup only – if at all)
SSH – vulnerable (off by default, should not be turned on)

Solution

As fixes become available for a given product, that information will appear in this bulletin in subsequent releases. Polycom will continue updating this bulletin until all fixes are in place. Polycom recommends that users of any Polycom product listed in the table above as being vulnerable update to the "FIXED" version of their product as soon as such a version becomes available.

CVSS v2 Base Metrics:

To assist our customers in the evaluation of this vulnerability; Polycom leverages the Common Vulnerability Scoring System (CVSS). This system provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities that better enable our customers to make informed decisions and assess the impact on their environment.

Base CVSS v2 Scores:

CVE-2014-6271: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVE-2014-7169: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

For more information on CVSS v2 please see:
http://www.first.org/cvss/cvss-guide.html

Severity: CRITICAL

Rating	Definition
Critical	A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.
High	A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources.
Medium	A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.
Low	A vulnerability that has minimal impact to the system and is extremely difficult to exploit.

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or visit:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

For the latest information. You might also find value in the high-level security guidance and security news located at:

http://www.polycom.com/security

Revision History

Revision 1.0 - Original publication: September 25, 2014 – First Announcement

Revision 1.1 – September 29, 2014 – More products added and **more CVE's added** to vulnerability details list

Revision 1.2 – ALL Polycom endpoints cleared, RMX 4000/2000/1500 cleared

Revision 1.3 – Legacy products added

Revision 1.4 – Detailed vulnerabilities of infrastructure products established at the vector level

Revision 1.5 – First fix announced, better dates and versions for fixes, better vector analysis

Revision 1.6 – OTX, RPX, SoundStructure all "not vulnerable". CloudAXIS, RPAD, RPRM vulnerability details updated. DMA fix announced.

Revision 1.7 – MGC and RSS 2000 added, not vulnerable